REMARKS

The specification has been amended to correct a typographical error.

Claims 1, 3-7, 10-16 and 18-20 have been rejected under 35 U.S.C. 102(e) as being anticipated by Wang (U.S. 6,175,922), and claims 2, 8, 9 and 17 have been rejected under 35 U.S.C. 103(a) as being unpatentable over Wang in view of Ladd et al. (U.S. 6,269,336).

The disclosure of Wang has been carefully reviewed, and the claims have been amended to further clarify this invention in light of the teachings of Wang.

Claims 1, 7 and 16 have been amended to emphasize that the method and system operate to automatically detect a presence of a message received from the commerce-related site that requires an authentication of the user as a response, and that the message sent to the mobile station is sent in "response to automatically detecting the presence of the message". Support for this amendment is found in the specification at least at page 10, lines 18-30, and page 12, lines 11-19. Reference is also made to Fig. 2, blocks B and C, and page 13, lines 26-30.

Wang is not seen to teach or suggest similar subject matter, and thus cannot anticipate these claims under 35 U.S.C. 102(e).

Dependent claim 21 has been added, and specifies that the received message is automatically detected using "message parsing". Support for this amendment is found at least page 10, lines 11-17.

In that claims 1, 7 and 16 are clearly patentable over Wang, then all claims that depend from claims 1, 7 and 16 should also be found to be patentable over Wang, whether considered alone or in combination with Ladd et al.

Note further that claim 9, as filed, recites in part that the "computer operates to prompt the user

to enter a personal identification number (PIN)", and that a "user authentication module in said mobile station compares the entered PIN to a PIN stored in the mobile station."

It is submitted that the Examiner's proposed combination of Wang and Ladd et al. does not suggest or disclose this subject matter.

Claim 9 has thus been re-written in independent form to include the subject matter found in claim 7, and to further specify that:

> "the computer operates to prompt the user to enter a personal identification number (PIN) into said computer, said computer transmits the entered PIN to said mobile station over the link, and where a user authentication module in said mobile station compares the entered PIN to a PIN stored in the mobile station". (emphasis added)

Support for this amendment can be found at least at page 18, lines 21-26.

Claim 9 is thus also believed to be clearly patentable over the proposed combination of Wang and Ladd et al.

Independent method claim 22 has been newly added, and refers in part to:

> "automatically detecting a presence of a received challenge from the site, the received challenge being detected based on message parsing that comprises Multi-Purpose Internet Mail Extensions (MIME) field recognition;
>
> in response to automatically detecting the presence of the received challenge, sending at least one message from the computer to the mobile station over a bidirectional wireless link;
>
> responsive to the receipt of the at least one message in the mobile station, generating a response to the challenge and transmitting the response to the computer over the link, where generating the response comprises prompting the user to enter personal identification information using one of a computer user interface or a mobile station user interface, and operating a user authentication module in the mobile station to validate the entered personal identification information; and

responsive to a receipt of the response at the computer, sending a response to the challenge to the site using the browser." (emphasis added)

Claim 22 is clearly patentable over the proposed combination of Wang and Ladd et al. for at least the reasons discussed above.

Independent method claim 23 has been newly added, and recites in part:

"automatically detecting a presence of a received request from the site;

in response to automatically detecting the presence of the received request, sending an inquiry to the mobile station from the computer for a list of certificates that are applicable to the request, the certificates being accessible by the mobile station;

presenting the list of applicable certificates to the user for selecting one of the presented certificates;

using the mobile station to communicate with a source of the selected certificate for completing the certificate;

passing the completed certificate to the browser; and

responsive to a receipt of the completed certificate, responding to the request received from the site." (emphasis added)

Dependent claim 24 further specifies that the request comprises "a request for an authenticated certificate, where the applicable certificates comprise authentication certificates, and where the completed certificate comprises an authenticated certificate", and dependent claim 25 further specifies that the request comprises "a request for a digital signature, where the applicable certificates comprise signature certificates, and where the completed certificate comprises a signed signature certificate." Support for these claims can be found at least at page 15, line 25, to page 16, line 31, and page 17, line 23, to page 18, line 20. Support for claim 28 can be found at least at page 16, lines 7-10 and 26-29. No new matter is entered.

Apparatus claim 30 is drawn to a mobile station. Claim 30 recites in part that the mobile station

can conduct communication with a server reachable through a data communications network, and includes a bidirectional data path for coupling to a network access application, and a controller, that is responsive to an automatic detection of a presence of a received request from the server by the access application or an extension of the access application, and to a reception of an inquiry from the access application, or the extension of the access application, for a list of mobile station accessible certificates that are applicable to the request, for returning the list of applicable certificates. In response to the user selecting one of the certificates, the controller communicates with a source of the selected certificate for completing the certificate and passes the completed certificate to the network access application for responding to the request received from the server.

Claims 31 and 32 are also newly added. Claim 31 recites in part that a method includes coupling an access application running on a computer to a server through a data communications network and "automatically detecting a presence of a request that is received from the server, the request being one that requires an authentication of a user". Claim 32 further defines the process of sending the message to the mobile station from the computer. All of these claims are patentable as well, for the reasons argued above with respect to claims 1-20.

An early notification of the removal of the rejections and the allowability of all of now pending claims 1-32 is earnestly solicited. The attached pages show the changes that were made to the claims.

ADDED PAGES TO SHOW CHANGES MADE

IN THE SPECIFICATION:

Rewrite the paragraph at page 6, lines 25-31, as follows:

The teachings of this invention go beyond only authenticating the user. For example, in the EMV environment a mobile station application, together with a peer application ~~ion~~ in the computer and optional transaction protocol(s) in the mobile station and the computer, can create a flow of operations for completing a financial transaction with a commerce related site.

IN THE CLAIMS:

Amend the claims as follows:

1. (Amended) A method for conducting electronic commerce, comprising steps of:

operating a computer to contact a commerce-related site using a browser;

automatically detecting a presence of a ~~received~~ message received from commerce-related site that requires, as a response, an authentication of a user;

in response to automatically detecting the presence of the message, sending a message from the computer to a mobile station over a link;

in response to receiving the message over the link, generating a user authentication message in the mobile station;

passing the user authentication message from the mobile station to the computer over the link; and

sending user authentication information to the commerce-related site using the browser.

5. (Amended) A method as in claim 1, wherein the steps of automatically detecting a

presence of the received message and sending the message from the computer to the mobile station include a step of operating an browser module.

7. (Amended) A system for conducting communication with a site reachable through a data communications network, comprising:

a mobile station comprising a user interface and a mobile station utilization application; and

a computer coupled to a data communications network and comprising a browser for contacting the site through the data communications network, the computer and browser operating to automatically detect a presence of a received message from the site that requires a response from the user, and further comprising an interface for sending a message from the computer to the mobile station over a bidirectional link in response to automatically detecting the presence of the message;

said mobile station utilization application being responsive to the receipt of the message from the link for generating a user response message and for passing the user response message to the computer over the link; and

said computer being responsive to a receipt of said user response message for sending user response information to the site using said browser.

9. (Amended) A system ~~as in claim 7~~ for conducting communication with a site reachable through a data communications network, comprising:

a mobile station comprising a user interface and a mobile station utilization application; and

a computer coupled to a data communications network and comprising a browser for contacting the site through the data communications network, the computer and browser

operating to automatically detect a presence of a received message from the site that requires a response from the user, and further comprising an interface for sending a message from the computer to the mobile station over a bidirectional link in response to automatically detecting the presence of the message;

said mobile station utilization application being responsive to the receipt of the message from the link for generating a user response message and for passing the user response message to the computer over the link; and

said computer being responsive to a receipt of said user response message for sending user response information to the site using said browser,

wherein said computer operates to prompt the user to enter a personal identification number (PIN) into said computer, said computer transmits the entered PIN to said mobile station over the link, and where a user authentication module in said mobile station compares the entered PIN to a PIN stored in the mobile station.

16. (Amended) A method for conducting communication with a site reachable through a data communications network, comprising steps of:

providing a mobile station having a user interface and an application;

coupling a computer to a data communications network, the computer having a browser for contacting the site through the data communications network;

automatically detecting with the computer a presence of a received message from the site that requires a response from the user;

in response to automatically detecting the presence of the received message, sending a message from the computer to the mobile station over a bidirectional link;

responsive to the receipt of the message in the mobile station, generating a user response message and passing the user response message to the computer over the link; and

responsive to a receipt of the user response message in the computer, sending user response information to the site using the browser.

Add the following new claims:

21. (New) A method as in claim 1, where the received message is automatically detected using message parsing.

22. (New) A method for conducting communication with a site reachable through the Internet, comprising:

providing a mobile station;

coupling a browser running on a computer to the site through the Internet;

automatically detecting a presence of a received challenge from the site, the received challenge being detected based on message parsing that comprises Multi-Purpose Internet Mail Extensions (MIME) field recognition;

in response to automatically detecting the presence of the received challenge, sending at least one message from the computer to the mobile station over a bidirectional wireless link;

responsive to the receipt of the at least one message in the mobile station, generating a response to the challenge and transmitting the response to the computer over the link, where generating the response comprises prompting the user to enter personal identification information using one of a computer user interface or a mobile station user interface, and operating a user authentication module in the mobile station to validate the

entered personal identification information; and

responsive to a receipt of the response at the computer, sending a response to the challenge to the site using the browser.

23. (New) A method for conducting communication with a site reachable through the Internet, comprising:

providing a mobile station;

coupling a browser running on a computer to the site through the Internet;

automatically detecting a presence of a received request from the site;

in response to automatically detecting the presence of the received request, sending an inquiry to the mobile station from the computer for a list of certificates that are applicable to the request, the certificates being accessible by the mobile station;

presenting the list of applicable certificates to the user for selecting one of the presented certificates;

using the mobile station to communicate with a source of the selected certificate for completing the certificate;

passing the completed certificate to the browser; and

responsive to a receipt of the completed certificate, responding to the request received from the site.

24. (New) A method as in claim 23, where the request comprises a request for an authenticated certificate, where the applicable certificates comprise authentication certificates,

and where the completed certificate comprises an authenticated certificate.

25. (New) A method as in claim 23, where the request comprises a request for a digital signature, where the applicable certificates comprise signature certificates, and where the completed certificate comprises a signed signature certificate.

26. (New) A method as in claim 23, where the received request is detected based on message parsing.

27. (new) A method as in claim 26, where message parsing comprises Multi-Purpose Internet Mail Extensions (MIME) field recognition

28. (New) A method as in claim 23, where completing the certificate comprises prompting the user to enter personal identification information using one of a computer user interface or a mobile station user interface, and verifying the entered personal identification information in cooperation with the source of the selected certificate.

29. (New) A method as in claim 23, where the list of applicable certificates are displayed to the user using one of a computer user interface or a mobile station user interface.

30. (New) A mobile station for conducting communication with a server reachable through a data communications network, comprising:

a bidirectional data path for coupling to a network access application; and

a controller, responsive to an automatic detection of a presence of a received request from the server by the access application or an extension of the access application, and to a reception of an inquiry from the access application, or the extension of the access application, for a list of mobile station accessible certificates that are applicable to the request, for returning the list of applicable certificates, and in response to the user selecting one of the certificates, for communicating with a source of the selected

certificate for completing the certificate and passing the completed certificate to the network access application for responding to the request received from the server.

31. (New) A method for conducting communication with a server, comprising:

coupling an access application running on a computer to the server through a data communications network;

automatically detecting a presence of a request that is received from the server, the request being one that requires an authentication of a user;

in response to automatically detecting the presence of the request, sending a message from the computer to a mobile station over a link;

in response to receiving the message over the link, generating a user authentication message in the mobile station;

passing the user authentication message from the mobile station to the computer over the link; and

sending user authentication information to the server using the access application.

32. (New) A method as in claim 31, where sending the message from the computer comprises sending an inquiry to the mobile station from the computer for a list of certificates that are applicable to the request, the certificates being accessible by the mobile station, and further comprising presenting the list of applicable certificates to the user for selecting one of the presented certificates; using the mobile station to communicate with a source of the selected certificate for completing the certificate; passing the completed certificate to the access application; and responsive to a receipt of the completed certificate, responding to the request received from the server.